R

Internetwork Security Monitor "ISM"

ISM and DIDS invalidate the indicated claims under 35 U.S.C. § 102(b) and 35 U.S.C. § 103*

All text citations are taken from:

L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, October 1992, pp. 262-271 ("ISM") [SYM_P_0069244- SYM_P_0069254]. SRI has admitted this paper was published before November 9, 1997. *See* SRI's Responses to Symantec's Third Set of RFAs, #48.

S.R. Snapp, J. Brentano, G.V. Dias, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, (with S.E. Smaha, T. Grance, D.M. Teal, D.L. Mansur), "DIDS -- Motivation, Architecture, and an Early Prototype" Proc. 14th National Computer Security Conference, Washington, DC, Oct. 1991, pp. 167-176 ("DIDS") [SYM_P_0077175- SYM_P_0077185]. SRI has admitted this paper was published before November 9, 1997. *See* SRI's Responses to Symantec's Third Set of RFAs, #19.

The text included herein are merely representative samples of the disclosure in the asserted reference. I reserve the right to supplement these disclosures.

<u>102(b)</u>

ISM invalidates the indicated claims under § 102(b). Additionally, *ISM* and *DIDS* constitute a single disclosure for purposes of 35 USC § 102(b) because *ISM* incorporates-by-reference the text of *DIDS*. *ISM* cites *to DIDS*. *See ISM* at 263, 264, 271. [SYM_P_0069245, SYM_P_0059246, SYM_P_0069253]. Furthermore, *ISM* explicitly states that ISM is an extension of DIDS:

> "Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks."

ISM at 264. [SYM_P_0069246].

<u>103</u>

In the alternative, *ISM* in combination with *DIDS* renders the indicated claims invalid due to obviousness under 35 USC § 103. The citations above provide a motivation to combine *ISM* and *DIDS* in order to extend DIDS to larger networks.

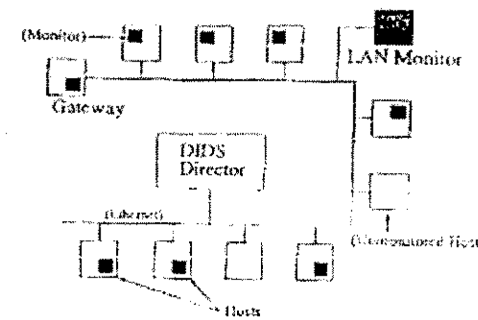
---

* 103 references are identified under the heading "**<u>103:</u>**".

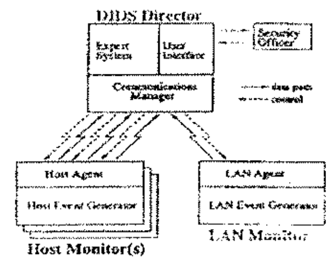
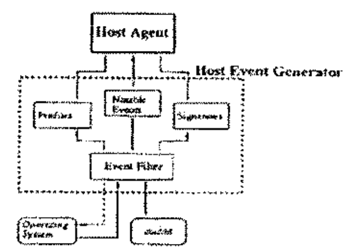
Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
1	A method of network surveillance, comprising:		"To address these limitations, we designed a model, called the Internetwork Security Monitor (ISM), to perform intrusion detection in a highly interconnected wide-area network." (263) [SYM_P_0069245] "In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture" (263) [SYM_P_0069245] "We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS's." (167) [SYM_P_0077175]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			 Fig. 1. Communications Architecture  Fig. 3. Host Monitor Structure [SYM_P_0077184]
	receiving network packets handled by a network entity;		"In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			different design alternatives for distributed-network traffic monitoring and analysis including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment." (263) [SYM_P_0069245] "The NSM, initially designed to detect intrusive activity across a local-area network (LAN), already augments DIDS' analysis capability by scrutinizing network activity into hosts which do not support host monitors. . ." (265) [SYM_P_0069245] "We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets		"We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250] "The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet Worm exploited a hole in the mail service)." (269) [SYM_P_0069251] "The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179]
	the at least one measure monitoring data transfers, errors, or network connections;		See '203 claim 1 "Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			network traffic patterns." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179] "[3] L.T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, 'A Network Security Monitor,' *Proc. 1990 Symposium on Research in Security and Privacy*, pp. 296-2304, Oakland, CA, May 1990." (175) [SYM_P_0077183]
	comparing at least one long-term and at least one short-term statistical profile; and		"The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet Worm exploited a hole in the mail service)." (269) [SYM_P_0069251] "The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179] "Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179] "[3] L.T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, 'A Network Security Monitor,' *Proc. 1990 Symposium on Research in Security and Privacy*, pp. 296-2304, Oakland, CA, May 1990." (175) [SYM_P_0077183]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.		"The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet Worm exploited a hole in the mail service)." (269) [SYM_P_0069251] "The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179] "Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179] "[3] L.T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber. 'A Network Security Monitor,' *Proc. 1990 Symposium on Research in Security and Privacy*, pp. 296-2304, Oakland, CA, May 1990." (175) [SYM_P_0077183]
2	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer commands		<u>**103**</u>: "Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) [SYM_P_0077177] "The host monitor consists of a *host event generator* (HEG) and a *host agent*. The HEG collects and analyzes audit records from the host's operating system. The audit records are scanned for

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			notable events, which are transactions that are of interest independent of any other records. These include, among others, failed events, user authentications, changes to the security state of the system, and any network access such as *rlogin* and *rsh*." (169) [SYM_P_0077177] "The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor." (168) [SYM_P_0077176] "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] *See* L. Todd Heberlein., "A Network Security Monitor – Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use). NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-79 to 4-80 [SYM_P_0075135-36]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			NFR. *See* Ranum et al., "Implementing a Generalized Tool for Network Monitoring," Proceedings of the Eleventh Systems Administration Conference (LISA '97), San Diego, CA, Oct. 1997 [SYM_P_0070720-28], 5-6 [SYM_P_0070725-26]. SNMP/RMON. *See* my expert report.
3	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer errors.		<u>103</u>: "The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor." (168) [SYM_P_0077176] "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176] "The host monitor is currently installed on Sun SPARCstations running SunOS 4.0.x with the Sun C2 security package [9].

Internetwork Security Monitor "ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			Through the C2 security package, the operating system produces audit records for virtually every transaction on the system. These transactions include file accesses, system calls, process executions, and logins. The contents of the Sun C2 audit record are: record type, record event, time, real user ID, audit user ID, effective user ID, real group ID, process ID, error code, return value, and label." (170) [SYM_P_0077178] "The host monitor consists of a *host event generator* (HEG) and a *host agent*. The HEG collects and analyzes audit records from the host's operating system. The audit records are scanned for *notable events*, which are transactions that are of interest independent of any other records. These include, among others, failed events, user authentications, changes to the security state of the system, and any network access such as *rlogin* and *rsh*." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection.

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] *See* L. Todd Heberlein, "A Network Security Monitor – Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use). NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-79 - 4-80 [SYM_P_0075135-36], 4-61 [SYM_P_0075117], 4-67 [SYM_P_0075123], 4-69 [SYM_P_0075125], 4-82 [SYM_P_0075138]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SNMP/RMON. *See* my expert report.

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
4	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer volume.		"The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179]
5	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.		"The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] *See* L. Todd Heberlein, "A Network Security Monitor – Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use).
6	The method of claim 1, wherein the measure monitors network connections by monitoring network connection denials.		<u>**103**</u>. "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-72 [SYM_P_0075128], 4-62 [SYM_P_0075118]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A [SYM_P_0078067-68]. SNMP/RMON. *See* my expert report.
7	The method of claim 1, wherein the measure monitors network connections by monitoring a correlation of network connections requests and network connection denials.		<u>**103**</u>: "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], [SYM_P_0074948-5282], 1-10 [SYM_P_0074983], 4-63 [SYM_P_0075119], C-4 to C-5 [SYM_P_0075215-16], 4-62 [SYM_P_0075118], 4-72 [SYM_P_0075128]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.
8	The method of claim 1, wherein the measure monitors errors by monitoring error codes included in a network packet.		**103**: "The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor." (168) [SYM_P_0077176] "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176] "The host monitor is currently installed on Sun SPARCstations running SunOS 4.0.x with the Sun C2 security package [9]. Through the C2 security package, the operating system produces audit records for virtually every transaction on the system. These transactions include file accesses, system calls, process executions, and logins. The contents of the Sun C2 audit record are: record type, record event, time, real user ID, audit user ID, effective user ID, real group ID, process ID, error code, return value, and label." (170) [SYM_P_0077178] "The host monitor consists of a *host event generator* (HEG) and a *host agent*. The HEG collects and analyzes audit records from the host's operating system. The audit records are scanned for *notable events*, which are transactions that are of interest independent of any other records. These include, among others, failed events, user authentications, changes to the security state of

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			the system, and any network access such as *rlogin* and *rsh*." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] *See* L. Todd Heberlein, "A Network Security Monitor – Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use).

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-67 [SYM_P_0075123], 4-82 [SYM_P_0075138]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SNMP/RMON *See* my expert report Jeremy Frank, "Artificial Intelligence and Intrusion Detection: Current and Future Directions," Proc. of the 17th National Computer Security Conference (1994) [SYM_P_0073569-80].
10	The method of claim 8 wherein an error code comprises an error code indicating a reason a packet was rejected.		<u>**103**</u>: "The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor." (168) [SYM_P_0077176] "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine,

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176] "The host monitor is currently installed on Sun SPARCstations running SunOS 4.0.x with the Sun C2 security package [9]. Through the C2 security package, the operating system produces audit records for virtually every transaction on the system. These transactions include file accesses, system calls, process executions, and logins. The contents of the Sun C2 audit record are: record type, record event, time, real user ID, audit user ID, effective user ID, real group ID, process ID, error code, return value, and label." (170) [SYM_P_0077178] "The host monitor consists of a *host event generator* (HEG) and a *host agent*. The HEG collects and analyzes audit records from the host's operating system. The audit records are scanned for *notable events*, which are transactions that are of interest independent of any other records. These include, among others, failed events, user authentications, changes to the security state of the system, and any network access such as *rlogin* and *rsh*." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] See '338 claim 5 *See* L. Todd Heberlein., "A Network Security Monitor – Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use). NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-67

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			[SYM_P_0075123]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856]. SNMP/RMON. *See* my expert report.
11	The method of claim 1, further comprising responding based on the determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.		"The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet Worm exploited a hole in the mail service)." (269) [SYM_P_0069251] "The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors." (169) [SYM_P_0077177] "We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful." (169-70) [SYM_P_0077177- SYM_P_0077178]
12	The method of claim 11, wherein responding comprises transmitting an event record to a network monitor.		See '203 claim 1 "Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks." (264) [SYM_P_0069246]
13	The method of claim 12, wherein transmitting the event record to a network monitor comprises transmitting the event record to a hierarchically higher network monitor.		See '203 claim 1 "Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks." (264) [SYM_P_0069246]
14	The method of claim 13, wherein transmitting the event record to a network monitor comprises transmitting the event record to a network monitor that receives event records from		See '203 claim 1 "Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks." (264) [SYM_P_0069246]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	multiple network monitors.		
15	The method of claim 14, wherein the monitor that receives event records from multiple network monitors comprises a network monitor that correlates activity in the multiple network monitors based on the received event records.		See '203 claim 1 "Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks." (264) [SYM_P_0069246] "For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it." (269) [SYM_P_0069251]
16	The method of claim 11, wherein responding comprises altering analysis of the network packets.		"The architecture also provides for bidirectional communication management tools as they become useful. This communication consists primarily of notable events and anomaly reports from the monitors. The director can also make request for more detailed information from the distributed monitors via a 'GET' directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a 'SET' directive." (169) [SYM_P_0077177] "Upon request, the LAN monitor is also able to provide a more detailed examination of any connection, including capturing every character crossing the network (i.e., a wire-tap). This capability can be used to support a directed investigation of a particular subject or object." (171) [SYM_P_0077179]

Internetwork Security Monitor "ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
17	The method of claim 11, wherein responding comprises severing a communication channel.		"We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful." (169-70) [SYM_P_0077177- SYM_P_0077178] **103**: CIDF. *See* Maureen Stillman, "Revised CIDF Documents" Oct. 6, 1997 [SYM_P_0071236-261], [SYM_P_0071247-48]. AIS. *See* William Hunteman, "Automated Information System—"AIS) Alarm System," Proc. of the 20th National Systems Security Conference (October 1997) [SYM_P_0526260 – SYM_P_0526271], 10 [SYM_P_0526269]. Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40 (ACM 1994) [SYM_P_0074513 – SYM_P_0074524], 235-37 [SYM_P_0074519-21].

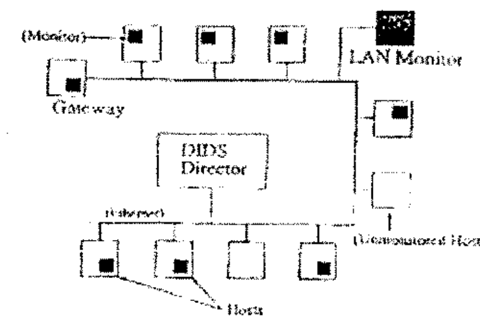
Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			'750 Patent. *See* U.S. Pat. No. 5,825,750 (Thompson) [SYM_P_0076772 – SYM_P_0076781], 5:63-6:6 [SYM_P_0076779]. synkill. *See* Schuba et al., "Analysis of a Denial of Service Attack on TCP," Proc. of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, 208-23 (May 4-7 1997) [SYM_P_0535408-28], 214-222 [SYM_P_0535419-27].
18	The method of claim 1, wherein the network packets comprise TCP/IP packets.		"GET CONNECTION TCP/IP-DEF <def> TIME <time> ... The second request (with the time given in the remote ISM's time frame) returns an identifier, which can be used to make further requests." (268) [SYM_P_0069250] "Because the Internet is distributed, evidence to identify and analyze an intrusion can be distributed over multiple sites on the Internet. Network managers at each site on the Internet must be provided with tools to analyze the evidence of an intrusion at the site and with tools to communicate their evidence and analysis with other managers so that the intrusion can be understood. The proposed ISM design focuses on providing a distributed, intelligent, decision-support system for network managers that would partially automate the detection of intrusions into the Internet." (270-271) [SYM_P_0069252- SYM_P_0069253]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			"The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179]
19	The method of claim 1, wherein the network entity comprises a gateway, a router, or a proxy server.		"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184]
21	A method of network surveillance, comprising:		See '338 claim 1
	monitoring network packets handled by a network entity;		See '338 claim 1

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	building a long-term and multiple short-term statistical profiles of the network packets;		See '338 claim 1
	comparing one of the multiple short-term statistical profiles with the long-term statistical profile; and		See '338 claim 1
	determining whether the difference between the one of the multiple short-term statistical profiles and the long-term statistical profile indicates suspicious network activity.		See '338 claim 1
24	A computer program product, disposed on a computer		See '338 claim 1

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	readable medium, the product including instructions for causing a processor to:		"Finally, security workbenches allow network managers to logon to their local ISM domain monitor to examine results of the monitor's analysis, query further into possible intrusions, exchange information with other network security managers, and administer various security tools such as Security Profile Inspector (SPI) or Computer Oracle Password Security System system (COPS)." (264) [SYM_P_0069246]
	receive network packets handled by a network entity;		See '338 claim 1
	build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets,		See '338 claim 1
	the measure monitoring data transfers, errors, or network connections;		See '338 claim 1
	compare at least one short-term and at least one long-term statistical profile; and		See '338 claim 1
	determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network		See '338 claim 1

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	activity.		
25	A method of network surveillance, comprising:		See '338 claim 1
	receiving packets at a virtual private network entity; and		**<u>103:</u>** SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856], 2-5 to 2-10 [SUN_000549-54]. NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 1-13 to 1-14 [SYM_P_0074986-87], B-10 to B-17 [SYM_P_0075204-11]. U.S. Patent No. 5,825,891 (Levesque) Key Management for Network Communication 10/29/1997 [SYM_P_0069852-SYM_P_0069866]
	building at least one long-term and at least one short-term statistical profile based on the received packets, and		See '338 claim 1
	comparing at least one long-term statistical profile with at least one short-term statistical profile to determine whether the packets indicate		See '338 claim 1

Internetwork Security Monitor
"ISM"

'338 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	suspicious network activity.		